November 9, 2018

VIA EMAIL:
privacyrfc2018@ntia.doc.gov

David J. Redl
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue N.W., Room 4725
Attn: Privacy RFC
Washington, DC 20230

Re: Developing the Administration's Approach to Consumer Privacy (83 FR 48600)[1]

Thank you for the opportunity to comment on the privacy protection framework under development by the National Telecommunications and Information Administration (NTIA). We very much appreciate the role of the NTIA in coordinating policy around commerce, technology, and access to the internet.

Mozilla is deeply invested in creating a healthy global internet, and the NTIA has a deep knowledge and critical role in protecting the internet. Creating privacy protections that people can trust is a core element of ensuring that the internet remains a global public resource. We have worked together fruitfully in the past and look forward to continuing to do so under your new leadership. We are glad that the Department of Commerce, and the NTIA, are exploring these important questions around privacy, transparency, and trust.

Mozilla is a global community of technologists, thinkers, and builders working together to keep the internet open, accessible, and secure. We are the creators of Firefox, an open source browser that hundreds of millions of people around the world use as their window to the web, as well as other products including Pocket, Focus, and Firefox Lite. To fulfill the mission of keeping the web open and accessible to all, we are constantly investing in the security of our products and the privacy of our users.

Through our policy and advocacy work, as a corporation, a foundation, and a global community, we focus on advancing key characteristics of the internet, from privacy to speech to innovation. We seek to build online trust so we can collectively create the Web our users want – the Web we all want. We also work towards other critical policy outcomes, from speech and misinformation to diversity and inclusion online. Our work attempts to find pragmatic, effective ways to protect the internet and ensure innovation is hand in hand with trust online.

[1] Accessible at https://www.federalregister.gov/d/2018-20941.

The privacy outcomes that your request outlines are an excellent start, and have strong historical grounding in the Fair Information Practices[2]. Additionally, a focus on outcomes - rather than on compliance checklists and specific legal mechanisms - is a good first step. We have seen, over time, that legalistic solutions often serve to create compliance checklists rather than strong privacy outcomes. It is also important to ensure that rules are not in conflict with other data protection regimes globally, in order to ensure the free flow of information.

Privacy and data at Mozilla

The web today is powered by user data. While that data has brought remarkable innovation and services, it has also put internet users at substantial risk. The data collection is accompanied by a constant risk of our social, financial, or political information being leaked in ways that expose us to harm. Data collection typically occurs without users' meaningful control or understanding. This has created a crisis of confidence in the internet.

It is clear that we are now at an inflection point, and that it is appropriate to reevaluate the framework by which the United States regulates the collection and use of personal data.

Mozilla has been committed to strong privacy protections, user controls, and security tools since we were founded. This commitment to security and privacy can be seen both in the open source code of our products as well as in our policies. Consider, for example, Mozilla's Data Privacy Principles[3] which guide the development of our products and services:

1. No surprises: Use and share information in a way that is transparent and benefits the user.
2. User Control: Develop products and advocate for best practices that put users in control of their data and online experiences.
3. Limited data: Collect what we need, de-identify where we can and delete when no longer necessary.
4. Sensible settings: Design for a thoughtful balance of safety and user experience.
5. Defense in depth: Maintain multi-layered security controls and practices, many of which are publicly verifiable.

This commitment is demonstrated throughout the product lifecycle. For example, Firefox - a web browser that runs on your device - serves as your gateway to the internet. Any browser manages a lot of information about the websites you visit, but that information can stay on your device. Mozilla, as the company that makes Firefox, doesn't collect that information unless you give us permission, and we will discuss some of the new tools we're building below.

---

[2] Gellman, Robert, Fair Information Practices: A Basic History (April 10, 2017). Available at SSRN: https://ssrn.com/abstract=2415020.

[3] Mozilla Data Privacy Principles, https://www.mozilla.org/en-US/privacy/principles/.

We do collect a set of data that helps us to understand how people use Firefox, called telemetry or analytics. We've purposely designed this data collection with privacy protections in mind. So while the browser knows a lot about you, Mozilla still knows very little - by design. Incentivizing this kind of thoughtful data collection and privacy by design should be one of the outcomes of these privacy principles.

Our Firefox data collection review process is the cornerstone of our effort to meaningfully practice privacy-by-design and assess privacy impacts to our users - a review process that should be a part of any thoughtful privacy design process.

Here are a few key pieces of that process:

- Before we look at any privacy risk, we need to know the analytic basis for the data collection. That is why our review process starts with a few simple questions about why Mozilla needs to collect the data, how much data is necessary, and what specific measurements will be taken. Mozilla employees who propose additional data collection must first answer these questions on our review form.
- Second, our Data Stewards – designated individuals on our Firefox team – will review the answers, ensure there is public documentation for data collection, and make sure users can turn data collection on and off.
- Third, we categorize data collection by different levels of privacy risk. The data category for the proposed collection must be identified as part of the review. For proposals to collect data in higher risk categories, the data collection must be turned off by default.
- Complex data collection requests, such as those to collect sensitive data or those that call for a new data collection mechanism, will escalate from our Data Stewards to our Trust and Legal teams. Further privacy, policy, and legal analysis will be done to assess privacy impact and identify appropriate mitigations.
- We publish the results of this review process, as well as in-depth descriptions of our data categories and the process itself.

This process is just one of the many tools we have to protect and empower the people who use our products. Last year, we rewrote our privacy notices to provide clear, simple language about the browser. The notice includes links directly to our Firefox privacy settings page, so users can turn off data collection if they read something on the notice they don't like.

Firefox Anti-Tracking

We also build privacy tools and features into our products, and just released new anti-tracking tools. We are working to put users back in control of their online privacy and to provide meaningful protections against tracking.

Firefox will protect users by blocking tracking while also offering a clear set of controls to give our users more choice over what information they share with sites. We are taking this approach after extensive research that shows users are not in control and do not fundamentally understand online tracking.

Opt-in privacy protections have fallen short. Firefox has always offered a baseline set of protections and allowed people to opt into additional privacy features. In parallel, Mozilla worked with industry groups to develop meaningful privacy standards, such as Do Not Track. However, these multi-stakeholder efforts have not been successful. Do Not Track has seen limited adoption by sites. Industry opt-outs don't always limit data collection, and often only forbid specific uses of the data.

The data collected by trackers is opaque to users and can create real harm. These are harms we cannot reasonably expect people to anticipate and take steps to avoid.

As the user agent, Firefox can help.

- Improving page load performance. Long page load times due to tracking content are detrimental to every user's experience on the web. For that reason, we've added a new feature in Firefox Nightly that blocks trackers that slow down page loads.
- Removing cross-site tracking. In order to help give users the private web browsing experience they expect and deserve, Firefox will strip cookies and block storage access from third-party tracking content. Our current plan is to turn this feature on by default when we release Firefox 65 in January.
- Mitigating harmful practices. We plan on blocking deceptive or malicious practices that abuse browser features for unintended purposes, such as fingerprinting and cryptomining.

Meaningful privacy frameworks

The initial framework for data privacy enumerated in this request for comment is a strong one, resting on well-understood Fair Information Privacy practices (FIPs). We support these FIPs, but encourage a more granular set of outcomes and goals to ensure that entities have adequate guidance to think through how to protect the privacy of their users - both in the United States and globally[4].

[4] For the purposes of this filing, we are using the term "privacy" in the traditional American sense: a broad overarching right that can mean different things in different contexts or to different people. It is worth exploring other terms, like "data protection," which are significantly less ambiguous. Data protection, a term used in the European Union, relates to the protection of individuals with regard to the processing of personal data, where 'processing' means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction including rules relating to the movement of personal data." (Article 4(2), GDPR) . While we are writing in support of a baseline privacy framework for the United States, we urge

Privacy, security, and data protection are well-served when policy is based upon a comprehensive framework of protections rather than solely technology or sector-specific regulations. Translating this framework into law, with FTC enforcement and rulemaking, is a necessary step to guide innovation and provide flexible guidance for new products and services. Given due respect and consideration to differences in products and business models, we believe that a purely technology or sector-specific approach risks creating an inconsistent patchwork of laws and could obscure the path forward for new technology. Moreover, all actors, both public and private, need to provide for user privacy and choice, and technology and sector-specific regulations risk the potential for gaps in protection and oversight. Adopting general standards also has the added benefit of providing a more future-proof approach, allowing new companies and entrepreneurs to understand and apply these standards as new technologies develop.

Privacy law in the United States is generally regarded as having fallen behind other national actors. Despite historical leadership on privacy globally as elaborated in the RFC, and strong sectoral laws - for example, in the financial industry - there is not a baseline rule that all data-driven entities need to follow. We support the existence of both a baseline rule as well as maintaining sectoral rules as contextually appropriate.

A strong baseline data privacy law would require the enshrinement of a robust framework of the rights of individuals with respect to both their data and the relationship with the entities that collect or use it. These entities - commonly called data controllers - should have significant responsibilities associated with the collection, storage, use, analysis, and processing of user data. And the law should have effective enforcement mechanisms via an empowered and independent regulator - in this case, the FTC.

A few elements of this framework are important to mention here:

- Covered entities - from all sectors - should be accountable to individuals and enforcement authorities for adhering to these principles. Covered entities should have an obligation to protect the security and privacy of personal data.
- Violations should be treated as unfair or deceptive acts and practices under the FTCA, with power to obtain civil penalties for wrongdoing.
- FTC should have the authority to promulgate rules pertinent to clarifying or implementing responsibilities on personal data.
- Personal data should only be collected, stored, used, and shared for purposes that an individual has consented to and for no longer than is necessary for the purposes for which it has been provided.
- Covered entities should offer individuals clear and simple choices, presented in a manner that enables individuals to make meaningful decisions about personal data.

---

specificity in terminology in order to help craft a legally sound framework which can be effectively implemented, and one which will help people understand - and enforce - their rights.

- Individuals should be able to exercise control over how covered entities use or share the personal data that is collected from and about them.
- Individuals should be able to correct the data describing them.
- Individuals should be provided understandable and comprehensive information describing the collection, storage, sharing, and use of personal data. Individuals should have access to the personal data that they have provided or generated through a service, and information about the decisions or profiling based on that personal data.
- Covered entities should notify the public and authorities regarding breaches of sensitive or personally-identifiable information, or other personal data that poses personal or financial risks, in a timely manner.
- In order to meet the reasonable expectations of individuals, any third parties that a covered entity provides personal data to must comply with the rights and preferences of individuals in the same manner as the first party.

Privacy outcomes

As previously discussed, the framework of privacy outcomes outlined in the RFC are founded upon the FIPs. In particular, we were pleased that NTIA highlighted the need for greater user control over the collection and use of personal information; minimization in the collection, storage, and use of data; and the implementation of security safeguards for personal information. In general, the outlined outcomes are consistent with well-established principles that organizations should use to design and implement data collection, as well as data driven products and services. Each of these is a worthwhile outcome, although more guidance may be necessary around the kinds of ways to operationalize them. For instance, privacy notices can take any number of forms, many of which - as the NTIA notes - are not helpful to most end users.

But while the FIPs provide a solid foundation for initial discussion, they also feature some notable shortcomings. The RFC acknowledges some of these issues, particularly in the context of notice-and-consent,[5] but there are other potential gaps that may arise during implementation of this outcome-based approach. In addition to the outcomes listed with in the RFC, the NTIA should consider including additional responsibilities and obligations for data controllers and codified in law to realize a right to privacy, including:

1. A right to object to the processing of personal data
2. Security and role-based access control and protections against unlawful disclosure
3. Training of employees and contractors

Right to Object to Processing of Personal Data

[5] Among other issues, notice-and-consent models shifts the burden of protecting their privacy from companies to users, many of whom may not read or understand the dense language featured in many privacy policies. Additionally, user control may not scale with too many granular options, and users may be unable to meaningfully consent to many potential uses of data.

The RFC explicitly refers for greater user control, specifying that users "should be able to exercise reasonable control over the collection, use, storage, and disclosure of the personal information they provide." And while user control is a fundamental principle of sound data privacy practices, further detail is needed to fully assess how effective this particular measure will be in practice. In particular, reasonable user control should also include the explicit right to object to the processing of personal data. This right will protect users when they are not provided with the opportunity to consent to the processing of their data, especially in the context of direct marketing.

While this principle is most commonly associated with European measures like the GDPR, there is substantial evidence that Americans could benefit from similar legal protections. For instance, Verizon tracked the internet activity of over 100 million users without their consent through "supercookies" that could not be deleted or circumvented.[6] As a result, Verizon was able to closely monitor the sites that users visited and catalogue their interests accordingly without their knowledge.[7] And although the FCC intervened and fined Verizon at the time,[8] the new leadership of the agency has since chosen to abdicate its authority to oversee data privacy practices under Section 222 of the Communications Act.[9] To prevent similar abuses of consumer privacy in the future, Congress should enshrine the rights of users into law and create an avenue to object to the processing of data in this manner.

Security and Role Based Access Control

In the context of security considerations, NTIA specifies within its principles that organizations should take "reasonable security measures" commensurate with the level of risk. While the RFC is largely focused on broad outcomes, we believe that the framework should specifically mandate security and role-based access controls (RBACs) and protections against unlawful disclosures. Broadly speaking, RBACs limit access to data based on the role that an employee serves within an organization.[10] Under this system, companies simply specify and enforce security policies that map naturally to the structure of the organization.[11] By managing access to

---

[6] *See* Craig Timberg, *Verizon, AT&T tracking their users with 'supercookies'*, Washington Post, Nov, 3, 2014, https://www.washingtonpost.com/business/technology/verizon-atandt-tracking-their-users-with-super-cookies/2014/11/03/7bbbf382-6395-11e4-bb14-4cfea1e742d5_story.html?utm_term=.d275117a9504; Jacob Hoffman-Andrews, *Verizon Injecting Perma-Cookies to Track Mobile Customers*, Bypassing Privacy Controls, Electronic Frontier Foundation (Nov. 3, 2014), https://www.eff.org/deeplinks/2014/11/verizon-x-uidh.

[7] Hoffman-Andrew, *supra* note 4.

[8] Consent Decree, In the Matter of Cellco Partnership, d/b/a Verizon Wireless (No. EB-TCD-14-00017601, FCC, March 7, 2016).

[9] *Restoring Internet Freedom*, WC Docket No. 17-108, Declaratory Ruling, Report and Order, and Order, 33 FCC Rcd 311 (2017).

[10] David F. Ferraiolo and D. Richard Kuhn, *Role-Based Access Controls*, 15th National Computer Security Conference at 554-563 (1992), available at https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1992/10/13/role-based-access-controls/documents/ferraiolo-kuhn-92.pdf.

[11] Michael Gallaher et al., The Economic Impact of Role-Based Access Control, RTI International (March 2002), available at https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=916549.

administrative systems and reducing employee delays for system access, this structure has been found to decrease the cost of network administration and improve the enforcement of network security policies.[12]

Training of Employees and Contractors

Part of this broader data privacy apparatus should also include proactive training of both employees and contractors regarding relevant data privacy laws, internal policies, and best practices for the handling of data. While employee awareness regarding specific domestic privacy laws like HIPAA seems to be relatively high, there appears to be lower levels of awareness concerning global privacy obligations that may be included in the GDPR and the Privacy Shield agreement.[13] With this in mind, employees may benefit from greater training to improve privacy literacy and close some of these gaps.

Global context

Globally, we see a consensus that baseline privacy protections are important, especially as more people use the internet for work, education, and the rest of their lives. We have advocated for strong privacy and data protection regulation during the legislative and regulatory process in Europe, South America, Africa, India, and at the state level in California - and there are other countries even now considering their data protection and privacy frameworks.

If some or all of the goals in the RFC are replicated by other countries - and many already are - this will provide global consistency. Conversely, adopting different approaches to privacy protection than other countries would introduce substantial capital and human resources costs on businesses wishing to go global who will need to build and maintain two systems to comply with these different legal frameworks. Ensuring that any baseline privacy framework in the United States is compatible with obligations globally would ease operations within the global context. It would also help the United States remain globally competitive - users of American products and services need to know that their data is being treated with respect, and the policies and laws that are put into place will determine how much trust they create within this ecosystem.

If the United States plans to lead on privacy, it must invest accordingly and codify comprehensive privacy protections in law. And while the high level principles in the RFC are relatively comprehensive, they also require more granular guidance in order to provide the certainty that companies should have as they design these products and services.

---

[12] *Id.*

[13] Thor Olavsrud, *Data privacy: What your employees don't know but should*, CIO, March 9, 2018, https://www.cio.com/article/3261946/privacy/data-privacy-what-your-employees-dont-know-but-should.html.

Federal Trade Commission authority and resources

Given its inherent structural limitations, the Federal Trade Commission (FTC) has done an admirable job protecting consumer privacy and regulating of technology and data driven companies more generally.

However, the FTC often runs into resource constraints or limits to their authority. Both of these can, and should, be rectified by Congress. Indeed, Chairman Simons highlighted some of these shortcomings and asked for additional FTC authority earlier this year in testimony before the Senate:

> "Section 5 … cannot address all privacy and data security concerns in the marketplace. For example, Section 5 does not provide for civil penalties, reducing the Commission's deterrent capability. The Commission also lacks authority over nonprofits and over common carrier activity, even though these acts or practices often have serious implications for consumer privacy and data security. Finally, the FTC lacks broad [Administrative Procedure Act] rulemaking authority for privacy and data security generally. The Commission continues to reiterate its longstanding bipartisan call for comprehensive data security legislation."[14]

First, the FTC lacks authority over several kinds of actors that handle significant amounts of personal information. Notably, telecommunications providers are exempt from FTC jurisdiction, despite having access to as much, if not more, sensitive personal data as large firms covered under sectoral federal privacy laws.[15] In this specific context, users would benefit from a joint approach to enforcement that (1) facilitates cooperation between the FCC and FTC and (2) provides the FTC with expanded enforcement authority.[16] Additionally, major nonprofits also fall within a similar gap in FTC oversight. These gaps should be resolved at a statutory level, ensuring that the data protection and privacy practices of common carriers and large nonprofits are clearly within FTC jurisdiction.

Second, the FTC's role in protecting privacy should also include the authority to hold rulemakings. The unique nature of the loss of private information justifies a prophylactic

---

[14] Hearing on Fiscal Year 2019 Funding Request and Budget Justification for the FCC and FTC Before the S. Subcomm. on Financial Services and General Government of the S. Comm. on Appropriations, 115th Cong. (2018) (statement of FTC Chairman Joseph Simons).

[15] *See* What ISPs Can See, Upturn (March 2016), available at https://www.upturn.org/reports/2016/what-isps-can-see/ ("Even with HTTPS, ISPs can still see the domains that their subscribers visit. This type of metadata can be very revealing, especially over time.").

[16] *Hearing on the FCC's Net Neutrality Rule Before the H. Comm. on the Judiciary*, 114th Cong. (2015) (statement of FTC Commissioner Terrell P. McSweeny) ("The optimum outcome for consumers is Open Internet [network rules] coupled with repeal of the common carrier exemption that may hinder the FTC from protecting consumers against unfair and deceptive common carrier activities. The FTC has decades of experience, and specific statutory tools such as consumer redress, that complement FCC oversight of common carriers.").

approach, as once this information is lost to the public, it is nearly impossible to regain exclusive control of it.[17] Expanding rulemaking authority will ensure that rules are flexible enough to address new threats and are informed by the significant expertise at the FTC. In particular, rulemaking could help the FTC stem out-of-context data collection, and ensure that the use and sharing of this data matches user expectations.[18] These rules could give users a much more meaningful understanding and expectation around the kinds of privacy protections they have.

Third, Section 5 of the FTC Act represents a relatively limited conception of stakeholder responsibility and consumer privacy.[19] To prove that an action is unfair under Section 5, the FTC must not only show that there was an injury, but also that the injury is not outweighed by a competitive or consumer benefit.[20] Under this model, privacy is merely a commodity weighed against other considerations, rather than a fundamental right.[21] In comparison, the standard under Section 222 of the Communications Act, which creates a duty for common carriers to shield the confidentiality of their customers, provides users with a more commensurate level of protection.[22]

Additionally, the FTC has repeatedly requested civil penalty authority to deter future violations of consumer privacy.[23] Because the agency currently lacks this ability, the FTC is largely dependent on consent decrees to impose penalties for privacy violations.[24] Under these settlements, an offender must first agree to terms and then subsequently violate the agreement before being penalized.[25] Moreover, these decrees frequently allow companies to satisfy its terms without improving internal privacy practices.[26] As a result, the current regime largely fails to deter bad actors, and users suffer from a lack of comprehensive protection. With this in mind, civil penalty authority would give the FTC another valuable enforcement tool to better protect user privacy.

However, this increase in authority should also be accompanied by more resources and staff for the FTC itself. The FTC has been increasingly tasked with protecting consumer privacy and

---

[17] In the Matter of Restoring Internet Freedom, WC Docket No. 17-108, Amended Comments of the Center of Democracy and Technology, at 16 (CDT Comments).
[18] *Competition and Consumer Protection in the 21st Century*, Project No. 18122001, Comments of Consumers Union, at 18 (CU Comments).
[19] CDT Comments at 15.
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *See* Press Release, Fed. Trade Comm'n, *FTC Testifies before House Energy and Commerce Subcommittee about Agency's Work to Protect Consumers, Promote Competition, and Maximize Resources* (July 18, 2018), https://www.ftc.gov/news-events/press-releases/2018/07/ftc-testifies-house-energy-commerce-subcommittee-about-agencys.
[24] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Columbia L. Rev. 583, 610 (2014).
[25] *Competition and Consumer Protection in the 21st Century*, Project No. 18122001, Comments of the Center for Democracy & Technology, at 8.
[26] *Id.* at 9-10.

security across many different industries, but the agency has a relatively limited staff to carry out this multifaceted mission. As Commissioner Rebecca Slaughter recently pointed out, while the economy has doubled in size since the Reagan administration, the FTC has fewer employees today than it did then.[27] And while data protection authorities abroad like the Information Commissioner's Office in the United Kingdom have over 500 staffers to handle complaints,[28] the FTC had only 54 full-time staffers in the Department of Privacy and Identity Protection to address threats in a rapidly growing and evolving field.[29] If the United States plans to lead on privacy, it must invest accordingly in more analysts, technologists, and attorneys at the FTC to demonstrate that commitment.

Supplementing the present framework for FTC authority laid out in Section 5 - useful though it is - will be necessary in order to better protect personal privacy.

In conclusion

Thank you for the opportunity to comment on the NTIA's privacy framework, including desired outcomes and goals. We are pleased to see the Administration seek broad comment from stakeholders at such an important point in time. The NTIA and Department of Commerce have a key role to play in policymaking the tech industry on consumer protection and privacy grounds, in partnership with the Federal Trade Commission and Congress.

We support both the adoption of high level principles and the enactment of specific legal obligations built on those principles to provide legal certainty for data driven entities, with the necessary flexibility as well.

This will lead to long-term benefits for the entire ecosystem, including the internet's users and small businesses. We would be pleased to continue discussing these critical issues.

Heather West
Senior Policy Manager, Americas
Mozilla Corporation

Ferras Vinh
Internet Policy Manager
Mozilla Corporation

---

[27] Hearing on Oversight of the Federal Trade Commission Before the H. Subcomm. on Digital Commerce & Consumer Protection of the H. Comm. on Energy & Commerce, 115th Cong. (2018) (oral testimony of Commissioner Rebecca Slaughter).
[28] "History of the Information Commissioner's Office," Information Commissioner's Office (last visited Nov. 5, 2018), https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/.
[29] 2018 FTC Congressional Budget Justification, available at https://www.ftc.gov/system/files/documents/reports/fy-2018-congressional-budget-justification/2018-cbj.pdf.